MULTIPLICATION OF MODULAR NUMBERS

ABSTRACT OF THE DISCLOSURE

A circuit for the implementation of modular multiplication of numbers comprises an alternative formulation of the algorithm first proposed by R.C. Montgomery..The modified Montgomery algorithm is implemented in one of a plurality of circuits comprising full adders, half adders, registers and gates.